

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

UNITED STATES OF AMERICA

Plaintiff,

VS.

ROLANDO SHACKELFORD

Defendant,

CASE NO. 07 CR 0852

Judge: Hon. Castillo

**MOTION TO SUPPRESS EVIDENCE**

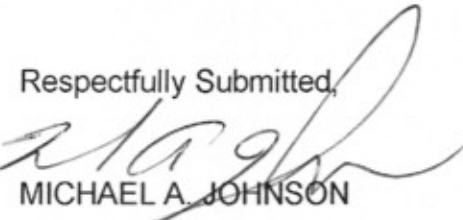
Now comes the Defendant, Rolando Shackelford, by and through his attorney Michael A. Johnson and moves this court to suppress from the introduction as evidence in this cause all evidence seized illegally from the defendant. In support of this Motion the Defendant state as follows:

1. That on December 19, 2002, agents from the United States Secret Service as well as other law enforcement officers entered the Defendants home located at 14611 Kilbourn, Midlothian, IL.
2. That at the time the agents and law enforcement officers entered the premises they were not in possession of a warrant to search the premises.
3. That neither the Defendant or any other individuals with authority, gave consent for the agents or any other law enforcement officers to enter or search the premises.
4. The search and seizure of the property was without probable cause.
5. That there were no exigent circumstances justifying a search without a warrant.
6. That after the search was completed and the evidence was seized, the agents produced a search warrant.

7. That the affidavit of Special Agent Paul A. Meyer recites that the information relied on to establish probable cause was obtained between the date of October 10, 1997 and January 11, 1998 ( see attached exhibit), whereas the warrant was not applied for until January 18, 2002. The excessive lapse of time involved rendered such information stale.

WHEREFORE, the Defendant, move this Court to grant this Motion, suppress from the introduction as evidence any and all property seized in violation of the Defendants constitutional rights.

Respectfully Submitted,



MICHAEL A. JOHNSON

Michael A. Johnson  
Attorney No. 51065  
415 N. LaSalle - Ste. 502  
Chicago, Illinois 60610  
312-222-0660  
[mjohnsonlawyer@aol.com](mailto:mjohnsonlawyer@aol.com)

- I, Franchon Foster, being duly sworn, state:
1. I own the property located at 14611 Kilbourn, Midlothian, IL. I owned that property on December 19, 2002.
  2. Rolando Shackelford also resided with me at 14611 Kilbourn, Midlothian, IL on December 19, 2002.
  3. In the morning hours of December 19, 2002 several police officers and agents came to my home.
  4. At the time that the agents and officers came, Rolando Shackelford was not at home. I told the officers that Mr. Shackelford was not here.
  5. I did not give consent to the officers or agents to enter my home or search my home. The agents never showed me a warrant of any kind.
  6. The officers and agents started to search my home and garage.
  7. I asked the agents if they had a search warrant and they could not produce one.
  8. I called my lawyer, Michael Johnson's office, I spoke to his secretary or answering service and asked them to have Mr. Johnson call me back.
  9. Mr. Johnson called me back. He asked me if I would hand the telephone to one of the agents. I heard Mr. Johnson ask the agent if he had a search warrant. The agent told Mr. Johnson he didn't need one, I heard Mr. Johnson tell the agent he needed a warrant or he would have to leave, at which point the agent handed me back the phone. Mr. Johnson told me to tell the agents they had to leave my home unless they had a search warrant.
  10. I asked the agents and officers to leave my home. The agent and officers refused to leave and continued to search my home and garage.
  11. The agents took property from my home, including computers and paperwork
  12. Just before the agents left my home they produced a search warrant. On the search warrant there was a time written on it, indicating 11:28 a.m.

Franchon Foster  
Franchon Foster

Date 3-5-08

Subscribed and sworn before me on 3-5-08

Isaac B Shapiro





Any and all evidence and instrumentalities of violation of Title 18, United States Code, Section 1029, found in the rear office or the garage at 14611 Kilbourn, Midlothian, Illinois, including, but not limited to:

1. Any and all records and documents relating to the manufacture and/or distribution of counterfeit credit cards and/or access devices.

2. Any and all records and documents relating to the production, distribution, and/or use of counterfeit access device.

3. Any and all records and documents listing names, addresses or credit card account numbers and/or bank account information of possible victims or suspects.

4. Any and all records and documents related to assets acquire by the use of proceeds obtained from the unlawful activity in violation of Title 18, United States Code, Sections 1029.

5. Any and all records and documents pertaining to the acquisition, transfer, concealment and expenditure of proceeds from the above-specified unlawful activities, including records, memoranda, letters, notes, invoices, records of real estate and personal property transactions, bank statements and related account records, financial statements, and loan applications.

6. The terms "records" and "documents" as used above include all of the foregoing items of evidence in whatever form and by whatever means such records, documents, their drafts, or their modifications may have been created or stored, including (but not limited to) any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs), or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, tapes, and printer buffers).

7. Any and all computer passwords and data security devices. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt,

8. Computers and computer records will be searched by means of an analysis of electronically stored data through several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the marking it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; or performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

9. Skimmers, encoders, the electronically stored content of encoders, the electronically stored content of computers, printers, fax machines, safes, the content of safes, scanners, typewriters, and cameras.

state as follows:

1. I am a Special Agent of the United States Secret Service and have been so employed for approximately one and one-half years. I am presently assigned to the Chicago office of the Secret Service. I investigate financial crimes, including credit card fraud. I have been trained in the investigation of fraudulent access device cases and in the use of computers, skimmers, encoders, scanners and other devices by people involved in the fraudulent use of access devices.

2. This affidavit is submitted in support of Application for search warrant for evidence of violations of Title 18, United States Code, Section 1029(a)(1).

3. The facts set forth below are based on my own personal knowledge, my review of investigative reports prepared by other law enforcement officers, and information provided by other law enforcement officers. Since this affidavit is submitted for the limited purpose of establishing probable cause, this affidavit does not contain a detailed account of everything that I know or other law enforcement officers know about the individual and events described herein. The affidavit sets forth only those facts, which I believe are necessary to establish the required probable cause.

4. On 10/10/1997, Detective Brad Borys, Lansing Police Department, provided the following information regarding



a. An individual cooperating with a local Police Department (hereinafter the "CI") related that an individual known to the CI as "Ro" was selling American Express credit cards for approximately \$1,000 USC, with a credit limit of approximately \$10,000.

b. The CI related "Ro" would even emboss the buyer's real name on the credit card.

c. The CI mentioned "Ro" showed him a blank green American Express credit card without the account number or the card member's name embossed on the credit card.

d. The CI recalled the front of the credit card had four numbers printed on the right side. The CI stated the numbers were "8673".

e. According to the CI, "Ro" was arrested on federal charges for cloning cellular telephones.

f. Johnson provided the following description for "Ro":  
Male/Black; 20-30 years old; 5'6" to 5'8"; 150-160lbs;  
Black hair, Box cut; wears a Mason ring;

Possible telephone numbers: Pager: 312/370-1480;

Work: 708/389-1609 IDH Financial Services, Midlothian, IL

g. On 11/12/1997, Secret Service conducted MCI record check reference Rolando Shackelford. Shackelford is of record with this Agency under case number 201-779-129084. Subject investigation is for cloning cellular telephones at L&A

5. On 10/14/1997, Joseph Gannon, Chief Investigator, World Financial Center, New York, NY, provided the following information concerning counterfeit credit cards with four digit batch code 1 also informed the Secret Service that on 10/20/1997, 201 Hammond Drive, Atlanta, GA, seized a counterfeit credit card with the 4DBC OF 8673, Account Number 9-81007, embossed in the name John Williams.

5. On 11/12/1997, Joseph Gannon relinquished counterfeit American Express credit cards with information of the above-mentioned credit cards in the possession of cards. While examining the counterfeit credit cards, the following investigative lead was developed:

a. On the upper right corner of the card is printed. ULTRA CARD II is the copyright trademark of the card systems produced by Fargo Electronics, MN.

7. On 11/12/1997, Jeffrey D. Upin, Legal Counsel, 7901 Flying Cloud Drive, Eden Prairie, MN, provided the following information:

a. Upin explained the ULTRA CARD II is a credit card with a mag strip on the reverse side of the card in conjunction with a digital computer printer to produce photo identification card



, Matteson, IL, were dispatched to the Foot  
11, Matteson, IL, to investigate the fraud  
t American Express credit card.

a. Officers learned from an employee of t  
a Black/Female, later identified as Angel  
n Express Credit card, account number 3732  
in the name Kristie Savage, to purchas  
e.

b. Powell presented the above-mentioned c  
: credit card receipt.

c. Powell was accomplished by a Bla  
l as Rolando Shackelford.

d. Powell and Shackelford were observe  
rether, with Shackelford carrying the  
se.

e. After Powell and Shackelford left t  
became suspicious of the transaction a  
Express for name and account number verifi

f. Manager learned the name and account  
e above-mentioned account number is liste

g. Powell and Shackelford were observed v  
level of the mall.

h. Powell and Shackelford were then observed walking in the same directions.

i. Powell was seen walking towards the upper level entrance of Carsons.

j. Shackelford was observed exiting the mall, carrying the merchandise via the lower level west parking lot.

k. Shackelford was observed entering the mall less than five minutes later without the merchandise.

On January 16, 1998, officers of the Matteson Police Department, Matteson, IL, arrested Rolando Shackelford and Angela Powell at the Lincoln Mall for fraudulent use of counterfeit American Express credit cards.

a. Powell was in possession of two (2) counterfeit American Express credit cards with the 4DBC OF 8673 embossed on the back and the name Kristie Savage.

b. Shackelford was in possession of one (1) counterfeit American Express credit card with the 4DBC OF 8673 embossed on the back and the name Robert Davis.

c. Examination of the above-mentioned cards revealed the words "ULTRA CARD II".

10. On 1/11/1998, Angela Powell was interviewed and advised that Shackelford had provided her with the fraudulent credit cards in the name of Kristie Savage, which she had used to purchase merchandise at the Foot Locker Store.

Grey Mercedes to the Lincoln mall parking lot. On January 22, 1998, a search warrant was executed on this vehicle which was opened with keys obtained from Shackelford. Among the items found in the vehicle were two computers. A subsequent search executed in February 1998 of these computers uncovered a computer file containing an image of the front of an American Express card with 4DBC of 8673 and another computer file containing an American Express Account number which had been embossed on a counterfeit American Express Card.

11. On December 19, 2002, at approximately 6:05 a.m., Secret Service agents including this affiant and local police officers knocked on the door at 14611 Kilbourn in Midlothian, Illinois. This affiant had spoken to Federal Probation Officer Jennifer Taborski on December 18<sup>th</sup>, and she informed me that Shackelford had been on probation until October 18, 2002 and lived with his wife at 14611 Kilbourn in Midlothian. Officer Toborski had added that this address is where she had done her home visits with Shackelford and is where Shackelford told her he lived.
12. After knocking on the door, Franchon Foster answered the door, acknowledged that she was Shackelford's wife, and agreed to allow the agents to enter and search the home

13. Upon entering a room in the rear of this one floor ranch home, this affiant and the other agents observed the following in plain view: two plastic access card reading devices known as skimmers; one encoder for DSS satellite systems, four portable computers and three computer monitors, two lap top computers, three laser jet printers, one fax machine, two document scanners, multiple cameras, various check software programs, a manual typewriter, a shredder, a safe, and numerous open boxes containing documents.
14. The one area the defendant's wife refused to let us view was the unattached garage which is located behind the home.
15. In light of the defendant's wife's refusal to allow access to the garage, in light of the other evidence described herein, my experience tells me that there is probable cause to believe that additional evidence of access fraud will be found in the garage. Moreover, I am aware through my experience and training that people engaged in access device fraud store documents and devices relating to their fraud in safes in their homes.
16. I have spoken this morning with Secret Service Special Agent Eric Dickey. Agent Dickey has previous training



and experience investigating access device fraud investigations involving the use of skimmers, encoders, computers, printers and scanners. Agent Dickey and I are aware through our experience and training that skimmers, encoders, computers, printers, fax machines and scanners are among the items used to facilitate the encoding or re-encoding of magnetic strips on credit cards and to keep track of the fraudulent credit card account numbers which are used. Moreover, scanners, typewriters, cameras and computers are used in the manufacture of fraudulent identification cards and access devices. In addition, encoders for DSS Satellite systems allow unauthorized users access to a DSS system without paying the provider. DSS systems are satellite TV systems which allow access to numerous television channels. In order to legally get this access, an individual must pay an authorized DSS provider for access. The use of encoders to obtain unauthorized access is a violation of 18 U.S.C. 1029 because it is unauthorized access to DSS systems.

Based on the foregoing, I believe that probable cause exists that the two plastic access card reading devices known as skimmers; the one encoder for DSS satellite systems, the four portable computers and three computer monitors, the two lap top computers, the electronically stored data contained in the computers, the three laser jet printers, the one fax machine, the two document scanners,

Case 1:07-cr-00852 Document 11 Filed 03/06/2008 Page 14 of 14  
the same as the Domain check program, the manual typewriter, the shredder, the safe, and the numerous open boxes containing documents, along with other documents, all contained within the rear office at the home, along with evidence of the above contained in the garage, contain fruits, instrumentalities and evidence relating to violations of Title 18, United States Code, Section 1029.

FURTHER AFFIANT SAYETH NOT

---

Paul A. Meyer, Special Agent  
United States Secret Service

Signed and Sworn to before me  
this 19<sup>th</sup> day of December, 2002



United States Magistrate Judge